(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－84274
（P2002－84274A）
(43)公開日　平成14年３月22日(2002.3.22)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
H04L	9/32		H04H	1/02	E　5C053
H04H	1/02		H04L	9/00	673B　5C064
H04N	5/91				675B　5J104
	7/167		H04N	5/91	P
				7/167	Z

審査請求　未請求　請求項の数11　ＯＬ　（全 11 頁）

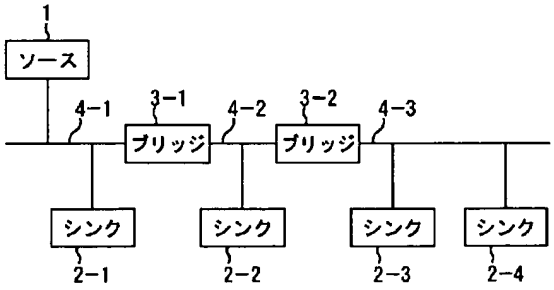
(21)出願番号　特願2000－211787(P2000－211787)
(22)出願日　平成12年７月12日(2000.7.12)
(31)優先権主張番号　特願2000－205615(P2000－205615)
(32)優先日　平成12年７月６日(2000.7.6)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　中野　雄彦
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082131
弁理士　稲本　義雄

Ｆターム(参考)　5C053 FA13 LA15
5C064 BA01 BB02 CA14 CB01 CC02 CC04
5J104 AA01 AA07 AA16 EA01 EA04 EA16 KA02 KA05 NA02 NA05 PA07

(54)【発明の名称】　情報処理装置および方法、並びに記録媒体

(57)【要約】
【課題】　コンテンツの利用を制限することができるようにする。
【解決手段】　ソース１は、シンク２－１よりコンテンツの送信要求を受けた場合、認証処理を行う。そして、認証に成功した場合、ソース１は、コンテンツにかけた暗号を解くのに必要な鍵情報をシンク２－１に送信する。シンク２－１は、鍵情報を受信し、それを使ってコンテンツにかけられた暗号を解くことにより、コンテンツを受信することができる。



【特許請求の範囲】
【請求項１】　ネットワークを介して他の装置にコンテンツを送信する情報処理装置において、
前記コンテンツを暗号化する暗号化手段と、
前記他の装置より受信許可が要求された場合、前記他の装置と認証する認証手段と、
前記認証手段の認証結果に基づいて、前記コンテンツの暗号を解除する解除鍵を前記他の装置に送信する送信手段と、
前記認証手段の認証結果に基づいて、前記他の装置の識別情報を取得する第１の取得手段と、
前記第１の取得手段により取得された前記識別情報に基づいて、前記コンテンツの受信台数を計数する第１の計数手段と、
前記第１の計数手段により計数された前記識別情報を記憶する記憶手段と、
前記第１の計数手段により計数された前記受信台数の値に基づいて、前記認証手段の認証の成否を制御することにより、前記コンテンツの受信台数を制御する制御手段とを備えることを特徴とする情報処理装置。
【請求項２】　前記認証手段の認証結果に基づいて、前記他の装置から受信台数の値を取得する第２の取得手段と、
前記第２の取得手段により取得された前記受信台数の値に基づいて、前記他の装置の受信台数を計数する第２の計数手段とをさらに備えることを特徴とする請求項１に記載の情報処理装置。
【請求項３】　前記送信手段により前記他の装置に送信された前記解除鍵が変更された場合、前記記憶手段により記憶された前記識別情報を消去するとともに、前記計数手段により計数された前記受信台数の値をリセットする情報更新手段をさらに備えることを特徴とする請求項１に記載の情報処理装置。
【請求項４】　ネットワークを介して他の装置にコンテンツを送信する情報処理装置の情報処理方法において、
前記コンテンツを暗号化する暗号化ステップと、
前記他の装置より受信許可が要求された場合、前記他の装置と認証する認証ステップと、
前記認証ステップの処理での認証結果に基づいて、前記コンテンツの暗号を解除する解除鍵を前記他の装置に送信する送信ステップと、
前記認証ステップの処理による認証結果に基づいて、前記他の装置の識別情報を取得する取得ステップと、
前記取得ステップの処理により取得された前記識別情報に基づいて、前記コンテンツの受信台数を計数する計数ステップと、
前記計数ステップの処理により計数された前記識別情報の記憶を制御する記憶制御ステップと、
前記計数ステップの処理により計数された前記受信台数の値に基づいて、前記認証ステップの処理での認証の成否を制御することにより、前記コンテンツの受信台数を制御する制御ステップとを含むことを特徴とする情報処理方法。
【請求項５】　ネットワークを介して他の装置にコンテンツを送信する情報処理装置用のプログラムにおいて、
前記コンテンツを暗号化する暗号化ステップと、
前記他の装置より受信許可が要求された場合、前記他の装置と認証する認証ステップと、
前記認証ステップの処理による認証結果に基づいて、前記コンテンツの暗号を解除する解除鍵を前記他の装置に送信する送信ステップと、
前記認証ステップの処理での認証結果に基づいて、前記他の装置の識別情報を取得する取得ステップと、
前記取得ステップの処理により取得された前記識別情報に基づいて、前記コンテンツの受信台数を計数する計数ステップと、
前記計数ステップの処理により計数された前記識別情報の記憶を制御する記憶制御ステップと、
前記計数ステップの処理により計数された前記受信台数の値に基づいて、前記認証ステップの処理での認証の成否を制御することにより、前記コンテンツの受信台数を制御する制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。
【請求項６】　第１のネットワークを介して第１の装置からコンテンツを受信する情報処理装置において、
前記第１の装置に対して、受信許可の要求を送信する第１の送信手段と、
前記第１の装置と認証する第１の認証手段と、
前記受信許可の要求を送信したとき、前記コンテンツの暗号を解除する解除鍵を、前記第１の装置から受信する受信手段と、
前記第１の装置から受信した前記コンテンツを、第２のネットワークを介して第２の装置に送信する第２の送信手段と、
前記第２の装置より受信許可が要求された場合、前記第２の装置と認証する第２の認証手段と、
前記第２の認証手段の認証結果に基づいて、前記受信手段により受信された前記解除鍵を前記第２の装置に送信する第３の送信手段と、
前記第２の認証手段の認証結果に基づいて、前記第２の装置の識別情報を取得する第１の取得手段と、
前記第１の取得手段により取得された前記識別情報に基づいて、前記コンテンツの受信台数を計数する第１の計数手段と、
前記第１の計数手段により計数された前記識別情報を記憶する記憶手段と、
前記第１の計数手段により計数された前記受信台数の値に基づいて、前記第２の認証手段の認証の成否を制御することにより、前記コンテンツの受信台数を制御する制

御手段とを備えることを特徴とする情報処理装置。
【請求項７】　前記コンテンツを復号する復号手段と、前記復号手段により復号された前記コンテンツを暗号化する暗号化手段とをさらに備えることを特徴とする請求項６に記載の情報処理装置。
【請求項８】　前記第１の認証手段の認証結果に基づいて、前記第１の計数手段により計数された前記受信台数の値を、前記第１の装置に送信する第４の送信手段と、前記第２の認証手段の認証結果に基づいて、前記第２の装置から受信台数の値を取得する第２の取得手段と、前記第２の取得手段により取得された前記受信台数の値に基づいて、前記第２の装置の受信台数を計数する第２の計数手段とをさらに備えることを特徴とする請求項６に記載の情報処理装置。
【請求項９】　前記第３の送信手段により前記第２の装置に送信された前記解除鍵が変更された場合、前記記憶手段により記憶された前記識別情報を消去するとともに、前記第１の計数手段により計数された前記受信台数の値をリセットする情報更新手段をさらに備えることを特徴とする請求項６に記載の情報処理装置。
【請求項１０】　第１のネットワークを介して第１の装置からコンテンツを受信する情報処理装置の情報処理方法において、
前記第１の装置に対して、受信許可の要求を送信する第１の送信ステップと、
前記第１の装置と認証する第１の認証ステップと、
前記受信許可の要求を送信したとき、前記コンテンツの暗号を解除する解除鍵を、前記第１の装置から受信する受信ステップと、
前記第１の装置から受信した前記コンテンツを、第２のネットワークを介して第２の装置に送信する第２の送信ステップと、
前記第２の装置より受信許可が要求された場合、前記第２の装置と認証する第２の認証ステップと、
前記第２の認証ステップの処理による認証結果に基づいて、前記受信ステップの処理により受信された前記解除鍵を前記第２の装置に送信する第３の送信ステップと、
前記第２の認証ステップの処理による認証結果に基づいて、前記第２の装置の識別情報を取得する取得ステップと、
前記取得ステップの処理により取得された前記識別情報に基づいて、前記コンテンツの受信台数を計数する計数ステップと、
前記計数ステップの処理により計数された前記識別情報の記憶を制御する記憶制御ステップと、
前記計数ステップの処理により計数された前記受信台数の値に基づいて、前記第２の認証ステップの処理での認証の成否を制御することにより、前記コンテンツの受信台数を制御する制御ステップとを含むことを特徴とする情報処理方法。
【請求項１１】　第１のネットワークを介して第１の装置からコンテンツを受信する情報処理装置用のプログラムにおいて、
前記第１の装置に対して、受信許可の要求を送信する第１の送信ステップと、
前記第１の装置と認証する第１の認証ステップと、
前記受信許可の要求を送信したとき、前記コンテンツの暗号を解除する解除鍵を、前記第１の装置から受信する受信ステップと、
前記第１の装置から受信した前記コンテンツを、第２のネットワークを介して第２の装置に送信する第２の送信ステップと、
前記第２の装置より受信許可が要求された場合、前記第２の装置と認証する第２の認証ステップと、
前記第２の認証ステップの処理による認証結果に基づいて、前記受信ステップの処理により受信された前記解除鍵を前記第２の装置に送信する第３の送信ステップと、
前記第２の認証ステップの処理による認証結果に基づいて、前記第２の装置の識別情報を取得する取得ステップと、
前記取得ステップの処理により取得された前記識別情報に基づいて、前記コンテンツの受信台数を計数する計数ステップと、
前記計数ステップの処理により計数された前記識別情報の記憶を制御する記憶制御ステップと、
前記計数ステップの処理により計数された前記受信台数の値に基づいて、前記第２の認証ステップの処理での認証の成否を制御することにより、前記コンテンツの受信台数を制御する制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、情報処理装置および方法、並びに記録媒体に関し、特に、コンテンツの利用を制限することができるようにした情報処理装置および方法、並びに記録媒体に関する。
【０００２】
【従来の技術】近年、インターネットに代表されるネットワークシステムが普及してきた。これにより、ユーザは、インターネットを介して情報を発信したり、あるいは、情報を受け取ったりすることができる。
【０００３】
【発明が解決しようとする課題】ところで、映画や音楽などの著作物の視聴を希望する利用者は、それに対する対価を支払うことにより、その著作物を受け取ることができる。
【０００４】しかしながら、インターネットなどのネットワークを通じて、映画や音楽などの著作物が、その所有者だけでなく、著作物に対する対価を支払っていない

多くの利用者に対して、不正に視聴されてしまう恐れがあった。

【０００５】また、ネットワークを通じて不正に視聴される行為が無制限に行われるようになると、コンテンツ作成および流通ビジネスを阻害する恐れがあった。

【０００６】本発明はこのような状況に鑑みてなされたものであり、コンテンツが、ネットワークを介して、不正に利用されるのを防止することができるようにするものである。

【０００７】

【課題を解決するための手段】本発明の第１の情報処理装置は、コンテンツを暗号化する暗号化手段と、他の装置より受信許可が要求された場合、他の装置と認証する認証手段と、認証手段の認証結果に基づいて、コンテンツの暗号を解除する解除鍵を他の装置に送信する送信手段と、認証手段の認証結果に基づいて、他の装置の識別情報を取得する第１の取得手段と、第１の取得手段により取得された識別情報に基づいて、コンテンツの受信台数を計数する第１の計数手段と、第１の計数手段により計数された識別情報を記憶する記憶手段と、第１の計数手段により計数された受信台数の値に基づいて、認証手段の認証の成否を制御することにより、コンテンツの受信台数を制御する制御手段とを備えることを特徴とする。

【０００８】本発明の第１の情報処理装置は、認証手段の認証結果に基づいて、他の装置から受信台数の値を取得する第２の取得手段と、第２の取得手段により取得された受信台数の値に基づいて、他の装置の受信台数を計数する第２の計数手段とをさらに設けるようにすることができる。

【０００９】本発明の第１の情報処理装置は、送信手段により他の装置に送信された解除鍵が変更された場合、記憶手段により記憶された識別情報を消去するとともに、計数手段により計数された受信台数の値をリセットする情報更新手段をさらに設けるようにすることができる。

【００１０】本発明の第１の情報処理方法は、コンテンツを暗号化する暗号化ステップと、他の装置より受信許可が要求された場合、他の装置と認証する認証ステップと、認証ステップの処理での認証結果に基づいて、コンテンツの暗号を解除する解除鍵を他の装置に送信する送信ステップと、認証ステップの処理による認証結果に基づいて、他の装置の識別情報を取得する取得ステップと、取得ステップの処理により取得された識別情報に基づいて、コンテンツの受信台数を計数する計数ステップと、計数ステップの処理により計数された識別情報の記憶を制御する記憶制御ステップと、計数ステップの処理により計数された受信台数の値に基づいて、認証ステップの処理での認証の成否を制御することにより、前記コンテンツの受信台数を制御する制御ステップとを含むことを特徴とする。

【００１１】本発明の第１の記録媒体に記録されているプログラムは、コンテンツを暗号化する暗号化ステップと、他の装置より受信許可が要求された場合、他の装置と認証する認証ステップと、認証ステップの処理での認証結果に基づいて、コンテンツの暗号を解除する解除鍵を他の装置に送信する送信ステップと、認証ステップの処理による認証結果に基づいて、他の装置の識別情報を取得する取得ステップと、取得ステップの処理により取得された識別情報に基づいて、コンテンツの受信台数を計数する計数ステップと、計数ステップの処理により計数された識別情報の記憶を制御する記憶制御ステップと、計数ステップの処理により計数された受信台数の値に基づいて、認証ステップの処理での認証の成否を制御することにより、前記コンテンツの受信台数を制御する制御ステップとを含むことを特徴とする。

【００１２】本発明の第１の情報処理装置、第１の情報処理方法、および第１の記録媒体に記録されているプログラムにおいては、コンテンツが暗号化され、他の装置より受信許可が要求された場合、その受信を許可しても受信台数が許容値を超えない限り、他の装置と認証され、その認証結果に基づいて、コンテンツの暗号を解除する解除鍵が他の装置に送信される。

【００１３】本発明の第２の情報処理装置は、第１の装置に対して、受信許可の要求を送信する第１の送信手段と、第１の装置と認証する第１の認証手段と、受信許可の要求を送信したとき、コンテンツの暗号を解除する解除鍵を、第１の装置から受信する受信手段と、第１の装置から受信したコンテンツを、第２のネットワークを介して第２の装置に送信する第２の送信手段と、第２の装置より受信許可が要求された場合、第２の装置と認証する第２の認証手段と、第２の認証手段の認証結果に基づいて、受信手段により受信された解除鍵を第２の装置に送信する第３の送信手段と、第２の認証手段の認証結果に基づいて、第２の装置の識別情報を取得する第１の取得手段と、第１の取得手段により取得された識別情報に基づいて、コンテンツの受信台数を計数する第１の計数手段と、第１の計数手段により計数された識別情報を記憶する記憶手段と、第１の計数手段により計数された受信台数の値に基づいて、第２の認証手段の認証の成否を制御することにより、コンテンツの受信台数を制御する制御手段とを備えることを特徴とする。

【００１４】本発明の第２の情報処理装置は、コンテンツを復号する復号手段と、復号手段により復号されたコンテンツを暗号化する暗号化手段とをさらに設けるようにすることができる。

【００１５】本発明の第２の情報処理装置は、第１の認証手段の認証結果に基づいて、第１の計数手段により計数された受信台数の値を、第１の装置に送信する第４の送信手段と、第２の認証手段の認証結果に基づいて、第

２の装置から受信台数の値を取得する第２の取得手段と、第２の取得手段により取得された受信台数の値に基づいて、第２の装置の受信台数を計数する第２の計数手段とをさらに設けるようにすることができる。

【００１６】本発明の第２の情報処理装置は、第３の送信手段により第２の装置に送信された解除鍵が変更された場合、記憶手段により記憶された識別情報を消去するとともに、第１の計数手段により計数された受信台数の値をリセットする情報更新手段をさらに設けるようにすることができる。

【００１７】本発明の第２の情報処理方法は、第１の装置に対して、受信許可の要求を送信する第１の送信ステップと、第１の装置と認証する第１の認証ステップと、受信許可の要求を送信したとき、コンテンツの暗号を解除する解除鍵を、第１の装置から受信する受信ステップと、第１の装置から受信したコンテンツを、第２のネットワークを介して第２の装置に送信する第２の送信ステップと、第２の装置より受信許可が要求された場合、第２の装置と認証する第２の認証ステップと、第２の認証ステップの処理による認証結果に基づいて、受信ステップの処理により受信された解除鍵を第２の装置に送信する第３の送信ステップと、第２の認証ステップの処理による認証結果に基づいて、第２の装置の識別情報を取得する取得ステップと、取得ステップの処理により取得された識別情報に基づいて、コンテンツの受信台数を計数する計数ステップと、計数ステップの処理により計数された識別情報の記憶を制御する記憶制御ステップと、計数ステップの処理により計数された受信台数の値に基づいて、第２の認証ステップの処理での認証の成否を制御することにより、コンテンツの受信台数を制御する制御ステップとを含むことを特徴とする。

【００１８】本発明の第２の記録媒体に記録されているプログラムは、第１の装置に対して、受信許可の要求を送信する第１の送信ステップと、第１の装置と認証する第１の認証ステップと、受信許可の要求を送信したとき、コンテンツの暗号を解除する解除鍵を、第１の装置から受信する受信ステップと、第１の装置から受信したコンテンツを、第２のネットワークを介して第２の装置に送信する第２の送信ステップと、第２の装置より受信許可が要求された場合、第２の装置と認証する第２の認証ステップと、第２の認証ステップの処理による認証結果に基づいて、受信ステップの処理により受信された解除鍵を第２の装置に送信する第３の送信ステップと、第２の認証ステップの処理による認証結果に基づいて、第２の装置の識別情報を取得する取得ステップと、取得ステップの処理により取得された識別情報に基づいて、コンテンツの受信台数を計数する計数ステップと、計数ステップの処理により計数された識別情報の記憶を制御する記憶制御ステップと、計数ステップの処理により計数された受信台数の値に基づいて、第２の認証ステップの処理での認証の成否を制御することにより、コンテンツの受信台数を制御する制御ステップとを含むことを特徴とする。

【００１９】本発明の第２の情報処理装置、第２の情報処理方法、および第２の記録媒体に記録されているプログラムにおいては、第１の装置より第１のネットワークを介して受信したコンテンツが、第１の装置より得た許可台数を上限に、第２のネットワークを介して第２の装置に送信される。

【００２０】

【発明の実施の形態】図１は、本発明を適用したネットワークシステムの構成例を示すブロック図である。このネットワークシステムにおいては、ソース１が、バス４－１を介して、シンク２－１およびブリッジ３－１に接続され、また、ブリッジ３－１が、バス４－２を介して、シンク２－２およびブリッジ３－２に接続され、さらに、ブリッジ３－２が、バス４－３を介して、シンク２－３，２－４に接続されている。

【００２１】ソース１は、コンテンツを出力する出力装置である。コンテンツを出力する場合、ソース１は、コンテンツを暗号化した後、バス４－１乃至４－３を介して、シンク２－１乃至２－４に出力する。なお、暗号化されたコンテンツの復号に必要な鍵情報は、認証処理に成功したシンクにだけ渡される。これにより、コンテンツを受信するシンクの台数が制限される。なお、後述するブリッジ３－１，３－２は、受信した信号を再出力するだけなので、台数カウントの対象から除外される。

【００２２】シンク２－１乃至２－４（以下、シンク２－１乃至２－４を個々に区別する必要がない場合、単にシンク２と記載する。その他の装置においても同様とする）は、ソース１より供給されたコンテンツを受信する受信装置である。認証処理に成功した場合、シンク２は、ソース１より渡された鍵情報に基づいて、受信したコンテンツを復号する。ただし、ブリッジ３－１や３－２が暗号を一旦解き、新たな鍵で暗号化して出力する場合は、シンク２－２乃至２－４は直接つながるブリッジより渡された鍵情報に基づいて、受信したコンテンツを復号する。

【００２３】ブリッジ３－１，３－２は、ソース１より出力された、暗号化されているコンテンツを受信し、復号した後、再び暗号化してシンク２－２乃至２－４に出力するものとする。そのため、ブリッジ３－１は、ソース１と認証処理を行い、暗号化されたコンテンツの復号に必要な鍵情報を取得するとともに、再出力するコンテンツを何台のシンク２に受信させたいかをソース１に伝える。そして、ブリッジ３－１は、ソース１から許可を得たら、ソース１に代わって、コンテンツを受信するシンク２－２乃至２－４の台数を制限する。なお、ブリッジ３－２は、ブリッジ３－１と認証し、同様にシンク２－３，２－４の受信台数を制限する。

【００２４】図２は、ソース１の詳細な構成例を示すブロック図である。

【００２５】コンテンツプレーヤ１１は、メディア１２が装着されると、制御部１５の制御に基づいて、メディア１２に記録されているコンテンツを再生し、暗号部１３に出力する。暗号部１３は、コンテンツプレーヤ１１より入力されたコンテンツを暗号化し、通信I/F（インタフェース）１４を介して、外部に出力する。なお、コンテンツプレーヤ１１とメディア１２の代わりに、放送コンテンツを受信し、出力するチューナーを持つソースも考えられる。

【００２６】制御部１５は、コンテンツプレーヤ１２、暗号部１３、通信I/F１４、および記憶部１６を制御する。制御部１５はまた、コンテンツプレーヤ１１で再生されたコンテンツを、必要に応じて、記憶部１６に記憶させる。

【００２７】図３は、シンク２の詳細な構成例を示すブロック図である。

【００２８】制御部２４は、画像・音声出力部２１、復号部２２、通信I/F２３、および、記憶部２５を制御する。制御部２４はまた、通信I/F２３を介して送信されてきた、暗号化されているコンテンツを復号部２２に送る。

【００２９】復号部２２は、通信I/F２３を介してソース１より送信されてきた鍵情報を取得する。復号部２２はまた、コンテンツを、取得した鍵情報に基づいて復号する。画像・音声出力部２１は、復号部２２で復号されたコンテンツを出力する。

【００３０】図４は、ブリッジ３の詳細な構成例を示すブロック図である。

【００３１】制御部３５は、通信I/F３１、復号部３２、暗号部３３、通信I/F３４、および、記憶部３６を制御する。制御部３５はまた、通信I/F３１を介して送信されてきた、暗号化されているコンテンツを復号部３２に送る。

【００３２】復号部３２は、通信I/F３１を介してソース１より送信されてきた鍵情報を取得するとともに、受信コンテンツを、取得した鍵情報に基づいて復号する。

【００３３】暗号部３３は、復号部３２で復号されたコンテンツを暗号化し、通信I/F３４を介して、外部に出力する。

【００３４】なお、認証には、公開鍵暗号技術を用いるものとし、ソース１、シンク２、およびブリッジ３は鍵管理組織が発行する各機器用のDigital Certificate（以下、Certificateと記載する）と各機器用の秘密鍵と鍵管理組織の公開鍵を持つものとする。このCertificateには各機器用の秘密鍵と対応する各機器用の公開鍵、その機器の固有ID、そしてこの２つのデータに対する鍵管理組織による電子署名が含まれるものとする。

【００３５】図５は、ソース１とシンク２－１（図１）が、直接接続される場合の認証処理を説明する図である。

【００３６】まず、シンク１が自分のCertificateをソース２－１に送信する。具体的には、シンク１の制御部１５が、記憶部１６からCertificateを読み出し、通信I/F１４を介して、ソース２－１に通信コマンドとして送信する（図５①）。

【００３７】ソース２は、この通信コマンドを受信すると、そのデータが正当なものか否かを判定する。具体的には、ソース２－１の制御部２４が、記憶部２５に記憶されている鍵管理組織の公開鍵を用いて、通信I/F２３を介して受信したCertificate中のデータと、それらに付随する鍵管理組織の電子署名が対応しているのか否かを調べる。すなわち、制御部２４は、公開鍵暗号のDSA（Digital Signature Algorithm）Verify演算処理を実行することにより、受信データの正当性を判定する。そして、判定結果が、正当である場合、認証処理を継続し、そうでない場合、認証処理を終了する。

【００３８】処理を継続する場合、ソース１の制御部１５は、Certificate中の相手のIDが記憶部１６に保持する認証済みIDリスト（以下、IDリストと記載する）に登録済みであるか否かを調べ、登録済みの場合、変数CntUpに０を代入する。

【００３９】一方、IDリストにCertificate中の相手のIDが未登録の場合、ソース１の制御部１５は、受信を許可したシンク２の数（以下、変数SinkCntと記載する）と受信を許可できる上限数（以下、変数MaxSinkと記載する）を比較し、変数SinkCntの方が小さければ変数CntUpに１を代入する。

【００４０】なお、SinkCnt＝MaxSinkの場合、認証処理は終了される。また、変数MaxSinkは、変数でなくてもよい（すなわち、定数であってもよい）。

【００４１】そして、ソース１の制御部１５は、擬似乱数生成アルゴリズムにより、擬似乱数Random_challengeを生成し、シンク２に通信コマンドとして送信する（図５②）。

【００４２】シンク２－１の制御部２４は、この通信コマンドを受信すると、その値に対して、記憶部２５に保持されている自分自身の秘密鍵を用いて、公開鍵暗号のDSASign演算処理を実行して、電子署名を計算する。シンク２－１の制御部２４は、計算された電子署名を、通信コマンド（Responseデータ）として、ソース１に送信する（図５③）。

【００４３】ソース１の制御部１５は、この通信コマンドを受信すると、自分が送った擬似乱数Random_challengeとこの電子署名が対応しているか否か、すなわち、上述したDSA Verify演算処理を実行して、データの正当性を判定する。ただし、ここでは、先の鍵管理組織の公開鍵の代わりに、相手から受け取ったCertificate中の相手の公開鍵が用いられる。そして、判定結果が、正当で

ある場合、認証処理が継続され、そうでない場合、認証処理は終了される。

【００４４】処理を継続する場合、ソース１の制御部１５は、コンテンツにかけた暗号を解くのに必要な鍵情報をシンク２－１に通信コマンドとして送信し（図５④）、変数SinkCntの値を変数CntUpの値だけ増加する。そして、ソース１の制御部１５は、Certificate中の相手のIDが記憶部１６に保持する認証済みIDリストに登録済みであるか否かを調べ、登録済みの場合、変数CntUpに０を代入する。一方、IDリストにCertificate中の相手のIDが未登録の場合、変数SinkCntと変数MaxSinkを比較し、変数SinkCntの方が小さければ変数CntUpに１を代入する。

【００４５】シンク２－１は、鍵情報を受信し、それを使ってコンテンツにかけられた暗号を解くことによって、コンテンツを受信することができる。

【００４６】また、図１に示されるソース１とシンク２－２のように、ソース１より出力されたコンテンツが、ブリッジ３－１を経由した後に、シンク２－２に受信される場合、やはり、シンク２－２とブリッジ３－１は、図５に示されたような認証処理を行う。すなわち、ソース１とシンク２－３、または、ソース１とシンク２－４のように、２台以上のブリッジ経由でコンテンツが伝送される場合でも、シンク１と最後のブリッジ３－２（シンク２－３，２－４と直接つながるブリッジ）は同様の認証処理を行う。

【００４７】以上の認証処理におけるシンク２の処理フローを図６に、ソース１の処理フローを図７に、それぞれ示す。

【００４８】シンク１の認証処理は、相手がブリッジ３であっても、ソース２の場合と全く同じである。ブリッジ３の認証処理は、図７のステップＳ１５に示す処理が、ソース２の場合と異なる。具体的には、SinkCnt＝MaxSinkの場合、ブリッジ３は、変数MaxSinkの値を大きくするために、自分自身が受信（入力）しているコンテンツの発信元であるソース１またはブリッジ３（図１の例の場合、ブリッジ３－１ならソース１、ブリッジ３－２ならブリッジ３－１）に受信許可を要求する認証処理を行う。なお、この場合には、１台以上の受信台数の追加が要求される。この認証処理が成功した場合、図７のステップＳ１６以降の処理が継続される。

【００４９】図８は、ソース１とブリッジ３－１（図１）が、直接接続される場合の認証処理を説明する図である。

【００５０】まず、ブリッジ３－１の制御部３５は、自分のCertificate、変数RelCntおよび変数AbsCntをソース１に送信する（図８①）。ここで、変数RelCntは、ブリッジ３－１が新たに得たい受信許可の台数を表わし、変数AbsCntは、既に得ている許可台数と今回許可を得たい台数の合計台数を表わしている。

【００５１】ソース１の制御部１５は、これを受信すると、Certificateが正当なものか否かを、上述したDSA Verify演算処理を実行することにより判定する。そして、判定結果が、正当でない場合、認証処理は終了される。

【００５２】処理を継続する場合、ソース１の制御部１５は、Certificate中の相手のIDが自分のIDリストに登録済みか否かを調べ、登録済みの場合、変数CntUpに変数RelCntを代入する。

【００５３】一方、IDリストにCertificate中の相手のIDが未登録の場合、ソース１の制御部１５は、変数CntUpに変数AbsCntを代入する。そして、ソース１の制御部１５は、変数SinkCntに変数CntUpを加えた値が、変数MaxSinkより小さいか否かを判定し、等しい場合、認証処理を終了する。

【００５４】そして、ソース１の制御部１５は、擬似乱数Random_challengeを生成し、ブリッジ３－１に通信コマンドとして送信する（図８②）。

【００５５】ブリッジ３－１の制御部３５は、この通信コマンドを受信すると、その値と送信済みの変数RelCntと変数AbsCntに対して、記憶部３６に保持されている自分自身の秘密鍵を用いて、上述したDSA Sign演算処理を実行して、電子署名を計算する。ブリッジ３－１の制御部３５は、計算された電子署名を、通信コマンド（Responseデータ）として、ソース１に送信する（図８③）。

【００５６】ソース１の制御部１５は、この通信コマンドを受信すると、自分が送った擬似乱数Random_challenge、受信済みの変数RelCntおよび変数AbsCntに、この電子署名が対応しているか否か、すなわち、上述したDSA Verify演算処理を実行して、データの正当性を判定する。ただし、ここでは、先の鍵管理組織の公開鍵の代わりに、相手から受け取ったCertificate中の相手の公開鍵が用いられる。そして、判定結果が、正当でない場合、認証処理は終了される。

【００５７】処理を継続する場合、ソース１の制御部１５は、コンテンツにかけた暗号を解くのに必要な鍵情報をブリッジ３－１に通信コマンドとして送信し（図８④）、変数SinkCntの値を変数CntUpの値だけ増加させた後、相手のIDがIDリストに未登録の場合、追加する。

【００５８】ブリッジ３－１は、鍵情報を受信し、それを使ってコンテンツにかけられた暗号を解いた後、再び暗号化してコンテンツを出力する。そして、ブリッジ３－１の制御部３５は、変数MaxSinkの値を変数RelCntの値だけ増加する。

【００５９】以上の認証処理におけるブリッジ３の処理フローを図９に、またソース１の処理フローを図１０に、それぞれ示す。

【００６０】また、図１に示されるソース１とシンク２－３、またはソース１とシンク２－４のように、ソース１より出力されたコンテンツが、２台以上のブリッジ３

－１，３－２を経由した後に、シンク２－３，２－４に受信される場合、やはり、コンテンツを出力するブリッジ３－１（以下、Txブリッジと記載する）とそれを受け取るブリッジ３－２（以下、Rxブリッジと記載する）は、図８に示されたような認証処理を行う。

【００６１】なお、Rxブリッジの認証処理は、相手がソース１の場合と全く同じである。

【００６２】Txブリッジの認証処理は、図１０のステップＳ４６に示す処理が、ソース１の場合と異なる。具体的には、SinkCnt＋CntUp＞MaxSinkの場合、Txブリッジは、変数MaxSinkの値を大きくするために、自分自身が入力しているコンテンツの発信元であるソース１またはブリッジ３に受信許可を要求する認証処理を行う（図１の例の場合、ブリッジ３－１はソース１に認証を要求する）。なお、この場合には（（SinkCnt＋CntUp）－MaxSink）以上の受信台数の追加が要求される。この認証処理が成功した場合、図１０のステップＳ５０以降の処理が継続される。

【００６３】また、他の処理例としては、変数RelCntおよび変数AbsCntが、Certificateとは別に送信される場合が考えられる。例えば、図８③に示されたResponseと共に送信する方法、あるいは、全く別の通信コマンドで送信する方法もある。

【００６４】また、図７のステップＳ１５、または、図１０のステップＳ４６において、ブリッジ３－１，３－２が、新たに接続されたソース１かブリッジ３と認証を行う場合、その結果によらず、その後の処理は継続しない方法もある。すなわち、新たな認証は、次回以降の認証を成功させるためのものと位置付けることができる。

【００６５】さらにまた、シンク２が自分の出力を受けるのを止め、暗号を解くのに必要な情報を失った場合、ソース１またはブリッジ３は、変数SinkCntをそのシンク２の分だけ減らすことができる。例えば、ソース１やブリッジ３がコンテンツにかける暗号の鍵情報を変更したら、シンク２は、自分自身の変数SinkCntを０にすることができる。

【００６６】以上のように、ソース１またはブリッジ３が、出力を受けられるシンク２の受信台数を制限するようにしたので、以下に示すような効果が得られる。

（１）コンテンツに関する権利者は、コンテンツの不正視聴や記録を未然に防ぐことができる。

（２）ブリッジを使って信号を再出力した場合でも、ソースは、ブリッジの先にいるシンクも含め、台数を制限することができる。

（３）台数の制限を機器固有のIDを使って行うことで、同じシンクが何度認証しても台数を誤って増やすことが無い。

（４）ブリッジが受信許可をソースや別のブリッジに要求する際に、受信台数の増加または減少分と受信合計台数を知らせることで、ソースや別のブリッジは、そのブリッジと認証したことがある場合、あるいは、認証したことがない場合のいずれにおいても、変数SinkCntを容易に、正しい値に変更することができる。

（５）公開鍵暗号技術を用いることで、機器固有IDや要求台数を、安全に他の機器に渡すことができ、かつ、正しい台数管理を行うことができる。

【００６７】上述した一連の処理は、ハードウエアにより実行させることもできるが、ソフトウエアにより実行させることもできる。一連の処理をソフトウエアにより実行させる場合には、そのソフトウエアを構成するプログラムが、専用のハードウエアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、記録媒体からインストールされる。

【００６８】この記録媒体は、コンピュータとは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク（フロッピディスクを含む）、光ディスク（CD-ROM(Compact Disk-Read Only Memory),DVD(Digital Versatile Disk)を含む）、光磁気ディスク（MD（Mini-Disk）を含む）、もしくは半導体メモリなどよりなるパッケージメディアにより構成されるだけでなく、コンピュータに予め組み込まれた状態でユーザに提供される、プログラムが記録されているROMやハードディスクなどで構成される。

【００６９】なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【００７０】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【００７１】

【発明の効果】以上のように、本発明の第１情報処理装置、第１の情報処理方法、および第１の記録媒体に記録されているプログラムによれば、コンテンツを暗号化し、他の装置より受信許可が要求された場合、その受信を許可しても受信台数が許容値を超えない限り、他の装置と認証し、その認証結果に基づいて、コンテンツの暗号を解除する解除鍵を他の装置に送信するようにしたので、コンテンツの利用を制限することが可能になる。

【００７２】また、本発明の第２の情報処理装置、第２の情報処理方法、および第２の記録媒体に記録されているプログラムによれば、第１の装置より第１のネットワークを介して受信したコンテンツを、第１の装置より得た許可台数を上限に、第２のネットワークを介して第２の装置に送信するようにしたので、出力コンテンツの受信装置を、得た許可台数に基づいて制限することが可能になる。

【図面の簡単な説明】

【図１】本発明を適用したネットワークシステムの構成例を示すブロック図である。

【図２】図１のソースの詳細な構成例を示すブロック図である。

【図３】図１のシンクの詳細な構成例を示すブロック図である。

【図４】図１のブリッジの詳細な構成例を示すブロック図である。

【図５】ソースまたはブリッジとシンクの認証処理を説明する図である。

【図６】シンクのソースまたはブリッジに対する認証処理を説明するフローチャートである。

【図７】ソースまたはブリッジのソースに対する認証処理を説明するフローチャートである。

【図８】ソースまたはTxブリッジのRxブリッジの認証処理を説明する図である。

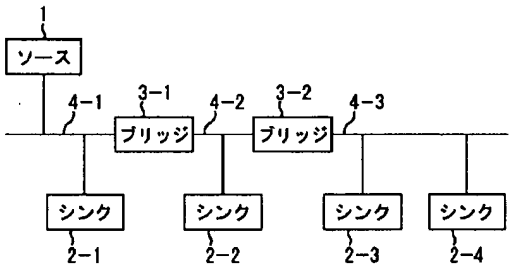
【図９】Rxブリッジのソースまたは Txブリッジに対する認証処理を説明するフローチャートである。

【図１０】ソースまたはTxブリッジのRxブリッジに対する認証処理を説明するフローチャートである。

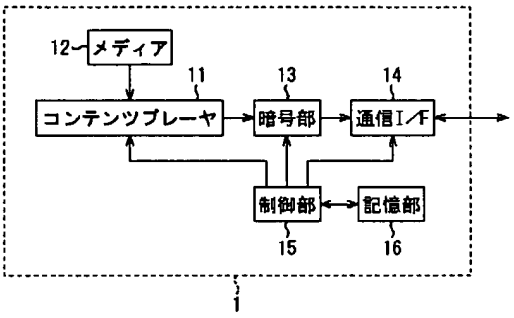
【符号の説明】

１　ソース，　２－１乃至２－４　シンク，　３－１，３－２　ブリッジ，１１　コンテンツプレーヤ，　１２　メディア，　１３　暗号部，　１４　通信I/F，　１５　制御部，　１６　記憶部，　２１　画像・音声出力部，　２２　復号部，　２３　通信I/F，　２４制御部，　２５　記憶部，　３１　通信I/F，３２　復号部，　３３　暗号部，　３４　通信I/F，　３５　制御部，　３６記憶部

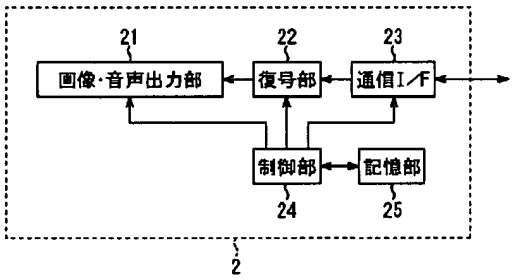
【図１】



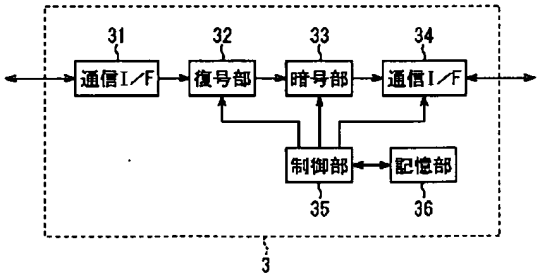
【図２】



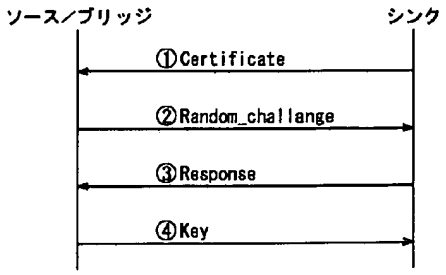
【図３】



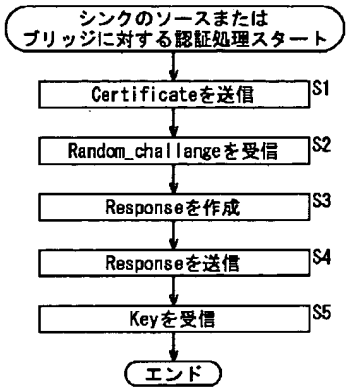
【図４】



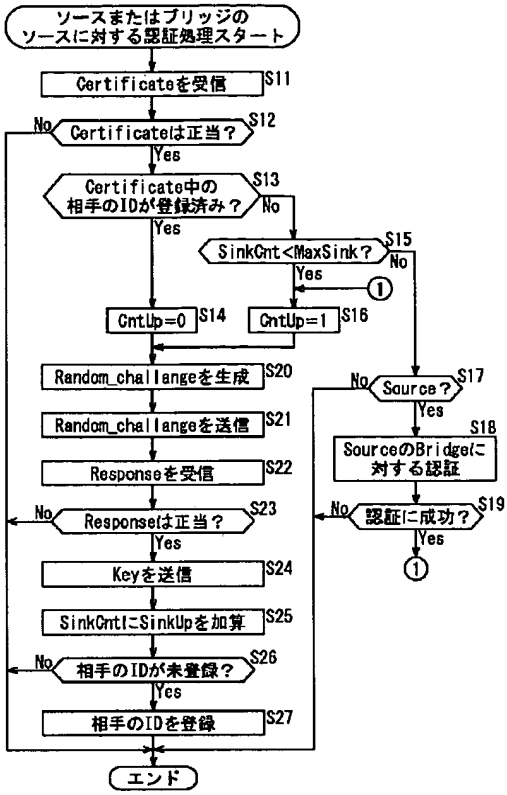
【図５】



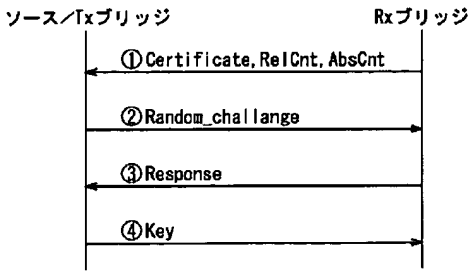
【図６】


シンクのソースまたは
ブリッジに対する認証処理スタート
Certificateを送信
S1
Random_challangeを受信
S2
Responseを作成
S3
Responseを送信
S4
Keyを受信
S5
エンド

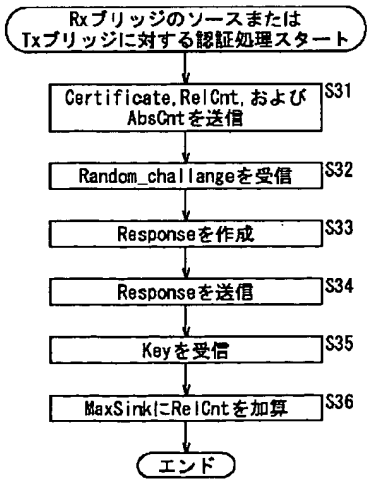
【図７】


ソースまたはブリッジの
ソースに対する認証処理スタート
Certificateを受信
S11
No
Certificateは正当？
S12
Yes
Certificate中の
相手のIDが登録済み？
S13
No
Yes
SinkCnt<MaxSink？
S15
No
Yes
①
CntUp=0
S14
CntUp=1
S16
Random_challangeを生成
S20
No
Source？
S17
Yes
SourceのBridgeに
対する認証
S18
No
認証に成功？
S19
Yes
①
Random_challangeを送信
S21
Responseを受信
S22
No
Responseは正当？
S23
Yes
Keyを送信
S24
SinkCntにSinkUpを加算
S25
No
相手のIDが未登録？
S26
Yes
相手のIDを登録
S27
エンド

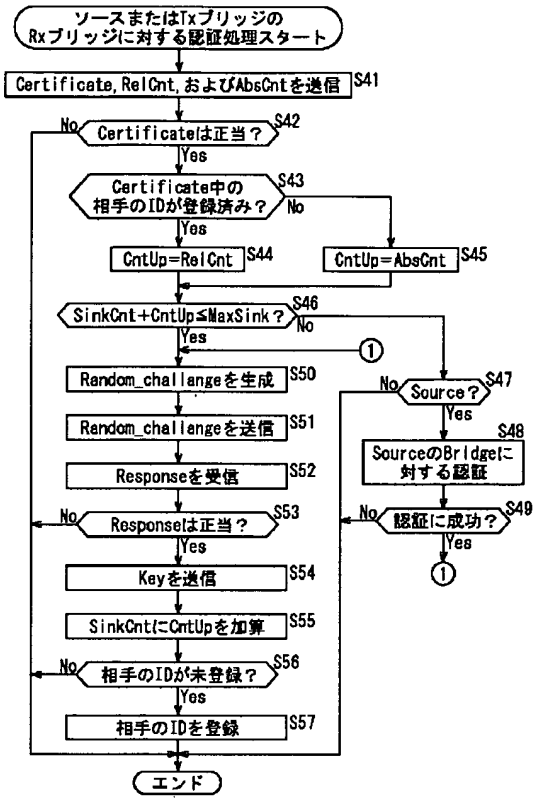
【図８】


ソース/Txブリッジ
Rxブリッジ
①Certificate, RelCnt, AbsCnt
②Random_challange
③Response
④Key

【図９】


Rxブリッジのソースまたは
Txブリッジに対する認証処理スタート
Certificate, RelCnt, および
AbsCntを送信
S31
Random_challangeを受信
S32
Responseを作成
S33
Responseを送信
S34
Keyを受信
S35
MaxSinkにRelCntを加算
S36
エンド

【図１０】


ソースまたはTxブリッジの
Rxブリッジに対する認証処理スタート
Certificate, RelCnt, およびAbsCntを送信
S41
No
Certificateは正当？
S42
Yes
Certificate中の
相手のIDが登録済み？
S43
No
Yes
CntUp=RelCnt
S44
CntUp=AbsCnt
S45
SinkCnt+CntUp≦MaxSink？
S46
No
Yes
①
Random_challangeを生成
S50
Random_challangeを送信
S51
Responseを受信
S52
No
Responseは正当？
S53
Yes
Keyを送信
S54
SinkCntにCntUpを加算
S55
No
相手のIDが未登録？
S56
Yes
相手のIDを登録
S57
エンド
No
Source？
S47
Yes
S48
SourceのBridgeに
対する認証
No
認証に成功？
S49
Yes
①

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-084274
(43)Date of publication of application : 22.03.2002

(51)Int.Cl. H04L 9/32
H04H 1/02
H04N 5/91
H04N 7/167

(21)Application number : 2000-211787
(22)Date of filing : 12.07.2000
(71)Applicant : SONY CORP
(72)Inventor : NAKANO KATSUHIKO

(30)Priority
Priority number : 2000205615 Priority date : 06.07.2000 Priority country : JP

(54) INFORMATION PROCESSING APPARATUS AND METHODAND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an information processing apparatus that can limit the utilization of contents.
SOLUTION: When receiving a contents transmission request from a sink 2-1a source 1 conducts authentication processing. When the source 1 is successful in the authenticationthe source 1 transmits key information required to decode the encryption applied to the contents. The sink 2-1 receives the key information and uses it to decode the encryption applied to the contents thereby receiving the contents.

CLAIMS

[Claim(s)]
[Claim 1]An information processor which transmits contents to other devices via a networkcomprising:
An encoding means which enciphers said contents.
An authentication means attested with a device besides the above when

reception permission is required from a device besides the above.
A transmitting means which transmits a release key of which a code of said contents is canceled to a device besides the above based on an authentication result of said authentication means.
The 1st acquisition means that acquires identification information of a device besides the above based on an authentication result of said authentication means.
The 1st counting means that calculates the number of receiving of said contents based on said identification information acquired by said 1st acquisition means.
A memory measure which memorizes said identification information calculated by said 1st counting means.
A control means which controls the number of receiving of said contents by controlling success or failure of attestation of said authentication means based on a value of said number of receiving calculated by said 1st counting means.

[Claim 2]The 2nd acquisition means that acquires a value of the number of receiving from a device besides the above based on an authentication result of said authentication meansThe information processor according to claim 1 having further the 2nd counting means that calculates the number of receiving of a device besides the above based on a value of said number of receiving acquired by said 2nd acquisition means.
[Claim 3]When said release key transmitted to a device besides the above by said transmitting means is changedwhile eliminating said identification information memorized by said memory measureThe information processor according to claim 1 having further an information updating means which resets a value of said number of receiving calculated by said counting means.
[Claim 4]An information processing method of an information processor which transmits contents to other devices via a network characterized by comprising the following.
An encryption step which enciphers said contents.
An authentication step attested with a device besides the above when reception permission is required from a device besides the above.
A transmission step which transmits a release key of which a code of said contents is canceled to a device besides the above based on an authentication result in processing of said authentication step.
An acquisition step which acquires identification information of a device besides the above based on an authentication result by processing of said authentication step.

A counting step which calculates the number of receiving of said contents based on said identification information acquired by processing of said acquisition step.
A storage control step which controls memory of said identification information calculated by processing of said counting step.
A control step which controls the number of receiving of said contents based on a value of said number of receiving calculated by processing of said counting step by controlling success or failure of attestation by processing of said authentication step.

[Claim 5]A program characterized by comprising the following for information processors which transmits contents to other devices via a network.
An encryption step which enciphers said contents.
An authentication step attested with a device besides the above when reception permission is required from a device besides the above.
A transmission step which transmits a release key of which a code of said contents is canceled to a device besides the above based on an authentication result by processing of said authentication step.
An acquisition step which acquires identification information of a device besides the above based on an authentication result in processing of said authentication step.
A counting step which calculates the number of receiving of said contents based on said identification information acquired by processing of said acquisition step.
A storage control step which controls memory of said identification information calculated by processing of said counting step.
A control step which controls the number of receiving of said contents based on a value of said number of receiving calculated by processing of said counting step by controlling success or failure of attestation by processing of said authentication step.

[Claim 6]An information processor which receives contents from the 1st device via the 1st networkcomprising:
The 1st transmitting means that transmits a demand of reception permission to said 1st device.
The 1st authentication means attested with said 1st device.
A reception means which receives a release key of which a code of said contents is canceled from said 1st device when a demand of said reception permission is transmitted.
The 2nd transmitting means that transmits said contents which received

from said 1st device to the 2nd device via the 2nd network.
The 2nd authentication means attested with said 2nd device when reception permission is required from said 2nd device.
The 3rd transmitting means that transmits said release key received by said reception means to said 2nd device based on an authentication result of said 2nd authentication means.
The 1st acquisition means that acquires identification information of said 2nd device based on an authentication result of said 2nd authentication meansThe 1st counting means that calculates the number of receiving of said contents based on said identification information acquired by said 1st acquisition meansA memory measure which memorizes said identification information calculated by said 1st counting meansand a control means which controls the number of receiving of said contents by controlling success or failure of attestation of said 2nd authentication means based on a value of said number of receiving calculated by said 1st counting means.

[Claim 7]The information processor according to claim 6 having further a decoding means which decodes said contentsand an encoding means which enciphers said contents decoded by said decoding means.
[Claim 8]The 4th transmitting means that transmits a value of said number of receiving calculated by said 1st counting means to said 1st device based on an authentication result of said 1st authentication meansThe 2nd acquisition means that acquires a value of the number of receiving from said 2nd device based on an authentication result of said 2nd authentication meansThe information processor according to claim 6 having further the 2nd counting means that calculates the number of receiving of said 2nd device based on a value of said number of receiving acquired by said 2nd acquisition means.
[Claim 9]When said release key transmitted to said 2nd device by said 3rd transmitting means is changedwhile eliminating said identification information memorized by said memory measureThe information processor according to claim 6 having further an information updating means which resets a value of said number of receiving calculated by said 1st counting means.
[Claim 10]An information processing method of an information processor which receives contents from the 1st device via the 1st network characterized by comprising the following.
The 1st transmission step that transmits a demand of reception permission to said 1st device.
The 1st authentication step attested with said 1st device.

A receiving step which receives a release key of which a code of said contents is canceled from said 1st device when a demand of said reception permission is transmitted.
The 2nd transmission step that transmits said contents which received from said 1st device to the 2nd device via the 2nd network.
The 2nd authentication step attested with said 2nd device when reception permission is required from said 2nd device.
The 3rd transmission step that transmits said release key received by processing of said receiving step to said 2nd device based on an authentication result by processing of said 2nd authentication step.
An acquisition step which acquires identification information of said 2nd device based on an authentication result by processing of said 2nd authentication stepA counting step which calculates the number of receiving of said contents based on said identification information acquired by processing of said acquisition stepA storage control step which controls memory of said identification information calculated by processing of said counting stepA control step which controls the number of receiving of said contents based on a value of said number of receiving calculated by processing of said counting step by controlling success or failure of attestation by processing of said 2nd authentication step.

[Claim 11]A program characterized by comprising the following for information processors which receives contents from the 1st device via the 1st network.
The 1st transmission step that transmits a demand of reception permission to said 1st device.
The 1st authentication step attested with said 1st device.
A receiving step which receives a release key of which a code of said contents is canceled from said 1st device when a demand of said reception permission is transmitted.
The 2nd transmission step that transmits said contents which received from said 1st device to the 2nd device via the 2nd network.
The 2nd authentication step attested with said 2nd device when reception permission is required from said 2nd device.
The 3rd transmission step that transmits said release key received by processing of said receiving step to said 2nd device based on an authentication result by processing of said 2nd authentication step.
An acquisition step which acquires identification information of said 2nd device based on an authentication result by processing of said 2nd authentication stepA counting step which calculates the number of

receiving of said contents based on said identification information acquired by processing of said acquisition stepA storage control step which controls memory of said identification information calculated by processing of said counting stepA control step which controls the number of receiving of said contents based on a value of said number of receiving calculated by processing of said counting step by controlling success or failure of attestation by processing of said 2nd authentication step.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]Especially this invention relates to the information processor and method of having enabled it to restrict use of contentsand a recording medium about an information processora methodand a recording medium.
[0002]
[Description of the Prior Art]In recent yearsthe network system represented by the Internet has spread. Therebythe user can disseminate information via the Internet or can receive information.
[0003]
[Problem(s) to be Solved by the Invention]By the waythe user who wishes viewing and listening of workssuch as a movie and musiccan receive the works by paying the remuneration to it.
[0004]Howeverthere was a possibility that it may be unjustly viewed and listened to workssuch as a movie and musicto many users who have not paid the remuneration not only to the owner but worksthrough networkssuch as the Internet.
[0005]When the act to which it is unjustly viewed and listened through a network came to be performed indefinitelythere was a possibility of checking contents creation and circulation business.
[0006]This invention is made in view of such a situationand it enables it to prevent contents from being unjustly used via a network.
[0007]
[Means for Solving the Problem]This invention is characterized by the 1st information processor comprising the following.
An encoding means which enciphers contents.
An authentication means attested with other devices when reception

permission is required from other devices.
A transmitting means which transmits a release key of which a code of contents is canceled to other devices based on an authentication result of an authentication means.
The 1st acquisition means that acquires identification information of other devices based on an authentication result of an authentication meansThe 1st counting means that calculates the number of receiving of contents based on identification information acquired by the 1st acquisition meansA memory measure which memorizes identification information calculated by the 1st counting meansand a control means which controls the number of receiving of contents by controlling success or failure of attestation of an authentication means based on a value of the number of receiving calculated by the 1st counting means.

[0008]The 1st information processor of this invention can establish further the 2nd acquisition means that acquires a value of the number of receiving from other devicesand the 2nd counting means that calculates the number of receiving of other devices based on a value of the number of receiving acquired by the 2nd acquisition means based on an authentication result of an authentication means.
[0009]It can establish further an information updating means which resets a value of the number of receiving calculated by a counting means while eliminating identification information memorized by a memory measurewhen the 1st information processor of this invention is changed [a release key transmitted to other devices by transmitting means].
[0010]This invention is characterized by the 1st information processing method comprising the following.
An encryption step which enciphers contents.
An authentication step attested with other devices when reception permission is required from other devices.
A transmission step which transmits a release key of which a code of contents is canceled to other devices based on an authentication result in processing of an authentication step.
An acquisition step which acquires identification information of other devices based on an authentication result by processing of an authentication stepA counting step which calculates the number of receiving of contents based on identification information acquired by processing of an acquisition stepA control step which controls the number of receiving of said contents by controlling success or failure of attestation by processing of an authentication step based on a value of the number of receiving calculated by processing of a storage control

step which controls memory of identification information calculated by processing of a counting stepand a counting step.

[0011]This invention is characterized by a program currently recorded on the 1st recording medium comprising the following.
An encryption step which enciphers contents.
An authentication step attested with other devices when reception permission is required from other devices.
A transmission step which transmits a release key of which a code of contents is canceled to other devices based on an authentication result in processing of an authentication step.
An acquisition step which acquires identification information of other devices based on an authentication result by processing of an authentication stepA counting step which calculates the number of receiving of contents based on identification information acquired by processing of an acquisition stepA control step which controls the number of receiving of said contents by controlling success or failure of attestation by processing of an authentication step based on a value of the number of receiving calculated by processing of a storage control step which controls memory of identification information calculated by processing of a counting stepand a counting step.

[0012]In the 1st information processor of this inventionthe 1st information processing methodand a program currently recorded on the 1st recording mediumUnless the number of receiving exceeds an acceptable value even if it permits the reception when contents are enciphered and reception permission is required from other devicesit is attested with other devices and a release key of which a code of contents is canceled is transmitted to other devices based on the authentication result.
[0013]This invention is characterized by the 2nd information processor comprising the following.
The 1st transmitting means that transmits a demand of reception permission to the 1st device.
The 1st authentication means attested with the 1st device.
A reception means which receives a release key of which a code of contents is canceled from the 1st device when a demand of reception permission is transmitted.
The 2nd transmitting means that transmits contents which received from the 1st device to the 2nd device via the 2nd networkThe 2nd authentication means attested with the 2nd device when reception permission is required from the 2nd deviceThe 3rd transmitting means

that transmits a release key received by a reception means to the 2nd device based on an authentication result of the 2nd authentication meansThe 1st acquisition means that acquires identification information of the 2nd device based on an authentication result of the 2nd authentication meansThe 1st counting means that calculates the number of receiving of contents based on identification information acquired by the 1st acquisition meansA memory measure which memorizes identification information calculated by the 1st counting meansand a control means which controls the number of receiving of contents by controlling success or failure of attestation of the 2nd authentication means based on a value of the number of receiving calculated by the 1st counting means.

[0014]The 2nd information processor of this invention can establish further a decoding means which decodes contentsand an encoding means which enciphers contents decoded by decoding means.
[0015]The 4th transmitting means that transmits a value of the number of receiving by which the 2nd information processor of this invention was calculated by the 1st counting means based on an authentication result of the 1st authentication means to the 1st deviceBased on an authentication result of the 2nd authentication meansthe 2nd acquisition means that acquires a value of the number of receiving from the 2nd deviceand the 2nd counting means that calculates the number of receiving of the 2nd device based on a value of the number of receiving acquired by the 2nd acquisition means can be established further.
[0016]When the 2nd information processor of this invention is changed [a release key transmitted to the 2nd device by the 3rd transmitting means]while eliminating identification information memorized by a memory measureAn information updating means which resets a value of the number of receiving calculated by the 1st counting means can be established further.
[0017]This invention is characterized by the 2nd information processing method comprising the following.
The 1st transmission step that transmits a demand of reception permission to the 1st device.
The 1st authentication step attested with the 1st device.
A receiving step which receives a release key of which a code of contents is canceled from the 1st device when a demand of reception permission is transmitted.
The 2nd transmission step that transmits contents which received from the 1st device to the 2nd device via the 2nd networkThe 2nd

authentication step attested with the 2nd device when reception permission is required from the 2nd deviceThe 3rd transmission step that transmits a release key received by processing of a receiving step to the 2nd device based on an authentication result by processing of the 2nd authentication stepAn acquisition step which acquires identification information of the 2nd device based on an authentication result by processing of the 2nd authentication stepA counting step which calculates the number of receiving of contents based on identification information acquired by processing of an acquisition stepA control step which controls the number of receiving of contents based on a value of the number of receiving calculated by processing of a storage control step which controls memory of identification information calculated by processing of a counting stepand a counting step by controlling success or failure of attestation by processing of the 2nd authentication step.

[0018]This invention is characterized by a program currently recorded on the 2nd recording medium comprising the following.
The 1st transmission step that transmits a demand of reception permission to the 1st device.
The 1st authentication step attested with the 1st device.
A receiving step which receives a release key of which a code of contents is canceled from the 1st device when a demand of reception permission is transmitted.
The 2nd transmission step that transmits contents which received from the 1st device to the 2nd device via the 2nd networkThe 2nd authentication step attested with the 2nd device when reception permission is required from the 2nd deviceThe 3rd transmission step that transmits a release key received by processing of a receiving step to the 2nd device based on an authentication result by processing of the 2nd authentication stepAn acquisition step which acquires identification information of the 2nd device based on an authentication result by processing of the 2nd authentication stepA counting step which calculates the number of receiving of contents based on identification information acquired by processing of an acquisition stepA control step which controls the number of receiving of contents based on a value of the number of receiving calculated by processing of a storage control step which controls memory of identification information calculated by processing of a counting stepand a counting step by controlling success or failure of attestation by processing of the 2nd authentication step.

[0019]In the 2nd information processor of this inventionthe 2nd

information processing methodand a program currently recorded on the 2nd recording mediumThe number of permission obtained from the 1st device is transmitted to contents which received via the 1st network from the 1st device by maximum via the 2nd network at the 2nd device.
[0020]
[Embodiment of the Invention]Drawing 1 is a block diagram showing the example of composition of the network system which applied this invention. In this network systemthe sauce 1 via the bus 4-1It is connected to the sink 2-1 and the bridge 3-1and the bridge 3-1 is connected to the sink 2-2 and the bridge 3-2 via the bus 4-2and the bridge 3-2 is further connected to sink 2-32-4 via the bus 4-3.
[0021]The sauce 1 is an output unit which outputs contents. When outputting contentsafter the sauce 1 enciphers contentsit is outputted to the sink 2-1 thru/or 2-4 via the bus 4-1 thru/or 4-3. Key information required for decoding of the enciphered contents is passed only to the sink which succeeded in authenticating processing. Therebythe number of a sink which receives contents is restricted. Since bridge 3-13-2 mentioned later only carries out the re output of the received signalit is excepted from the object of a number count.
[0022]The sink 2-1 thru/or 2-4 (hereafterwhen the sink 2-1 thru/or 2-4 do not need to be distinguished separatelyit is only indicated as the sink 2.) in other devices -- the same -- carrying out -- it is a receiving set which receives the contents supplied from the sauce 1. When it succeeds in authenticating processingthe sink 2 decodes the contents which received based on the key information passed from the sauce 1. Howeverthe bridge 3-1 and 3-2 once solve a codeand when enciphering and outputting with a new keythe sink 2-2 thru/or 2-4 decode the contents which received based on the key information passed from the bridge connected directly.
[0023]After bridge 3-13-2 receives and decodes the contents which were outputted from the sauce 1 and which are encipheredit shall encipher again and it shall be outputted to the sink 2-2 thru/or 2-4.
Thereforethe bridge 3-1 tells the sinks 2 he wants how many sets of to receive the contents which carry out a re output to the sauce 1 while it performs the sauce 1 and authenticating processing and acquires key information required for decoding of the enciphered contents. And the bridge 3-1 will restrict the sink 2-2 thru/or the number of 2-4 which receives contents instead of the sauce 1if permission is obtained from the sauce 1. The bridge 3-2 is attested with the bridge 3-1and restricts the number of receiving of sink 2-32-4 similarly.
[0024]Drawing 2 is a block diagram showing the detailed example of

composition of the sauce 1.
[0025]If equipped with the media 12the content player 11 will reproduce the contents currently recorded on the media 12 based on control of the control section 15and will output them to the cryptopart 13. The cryptopart 13 enciphers the contents inputted from the content player 11and outputs them outside via communication I/F(interface) 14. The sauce which receives broadcast contents and has a tuner to output instead of the content player 11 and the media 12 is also considered.
[0026]The control section 15 controls the content player 12the cryptopart 13communication I/F14and the storage parts store 16. The control section 15 makes the storage parts store 16 memorize again the contents reproduced with the content player 11 if needed.
[0027]Drawing 3 is a block diagram showing the detailed example of composition of the sink 2.
[0028]The control section 24 controls a picture and the voice output part 21the decoding part 22communication I/F23and the storage parts store 25. The control section 24 sends the contents which have been transmitted via communication I/F23 and which are enciphered to the decoding part 22 again.
[0029]The decoding part 22 acquires the key information transmitted from the sauce 1 via communication I/F23. The decoding part 22 decodes contents again based on the acquired key information. An image and the voice output part 21 output the contents decoded by the decoding part 22.
[0030]Drawing 4 is a block diagram showing the detailed example of composition of the bridge 3.
[0031]The control section 35 controls communication I/F31the decoding part 32the cryptopart 33communication I/F34and the storage parts store 36. The control section 35 sends the contents which have been transmitted via communication I/F31 and which are enciphered to the decoding part 32 again.
[0032]The decoding part 32 decodes receiving contents based on the acquired key information while acquiring the key information transmitted from the sauce 1 via communication I/F31.
[0033]The cryptopart 33 enciphers the contents decoded by the decoding part 32and outputs them outside via communication I/F34.
[0034]Digital Certificate for each apparatus by which a lock management organization publishes the sauce 1the sink 2and the bridge 3 for attestation using public-key-encryption art. It shall have a secret key for each apparatus (hereafter indicated to be Certificate)and a public key of a lock management organization. The electronic signature by the lock management organization to the secret key for each apparatusthe

corresponding public key for each apparatuspeculiar ID of that apparatusand these two data shall be included in this Certificate.
[0035]Drawing 5 is a figure explaining authenticating processing in case direct continuation of the sauce 1 and the sink 2-1 (drawing 1) is carried out.
[0036]Firstthe sink 1 transmits its Certificate to the sauce 2-1. The control section 15 of the sink 1 reads Certificate from the storage parts store 16andspecificallytransmits to the sauce 2-1 as a communication command via communication I/F14 (drawing 5 **).
[0037]The sauce 2 will judge whether it is a thing with that just dataif this communication command is received. It is investigated whether it is that the data in Certificate which the control section 24 of the sauce 2-1 specifically received via communication I/F23 using the public key of a lock management organization memorized by the storage parts store 25and the electronic signature of the lock management organization which accompanies them correspond. That isthe control section 24 judges the justification of received data by performing DSA(Digital Signature Algorithm) Verify data processing of public key encryption. And when a decision result is justauthenticating processing is continuedand when that is not rightit ends authenticating processing.
[0038]When continuing processingthe control section 15 of the sauce 1 investigates whether it is registered to the attested ID list (it is hereafter indicated as an ID list) which ID of the partner in Certificate holds to the storage parts store 16and when registeredit substitutes zero for the variable CntUp.
[0039]When ID of the partner in Certificate is unregisteredon the other handto an ID list the control section 15 of the sauce 1The number of the sinks 2 which permitted reception (it is hereafter indicated as the variable SinkCnt) is compared with the upper limit number (it is hereafter indicated as the variable MaxSink) which can permit receptionand one will be substituted for the variable CntUp if the variable SinkCnt is smaller.
[0040]In SinkCnt=MaxSinkauthenticating processing is ended. The variable MaxSink may not be a variable (that isit may be a constant).
[0041]And with a pseudorandom-numbers generation algorithmthe control section 15 of the sauce 1 generates pseudorandom-numbers Random_challengeand transmits to the sink 2 as a communication command (drawing 5 **).
[0042]The control section 24 of the sink 2-1 will calculate an electronic signature by performing DSASign data processing of public key encryption to that value using its own secret key currently held at the

storage parts store 25if this communication command is received. The control section 24 of the sink 2-1 transmits the calculated electronic signature to the sauce 1 as a communication command (Response data) (drawing 5 **).

[0043]If this communication command is receivedthe control section 15 of the sauce 1 will perform whether pseudorandom-numbers Random_challenge which he sentand this electronic signature correspondand DSAVerify data processing mentioned aboveand will judge the justification of data. Howeverthe public key of the partner in Certificate received from the partner is used instead of the public key of a previous lock management organization here. And when a decision result is justauthenticating processing is continuedand authenticating processing is ended when that is not right.

[0044]When continuing processingthe control section 15 of the sauce 1 transmits key information required to solve the code enciphered contents as a communication command to the sink 2-1 (drawing 5 **)and only the value of the variable CntUp increases the value of the variable SinkCnt. And the control section 15 of the sauce 1 investigates whether it is registered to the attested ID list which ID of the partner in Certificate holds to the storage parts store 16and when registeredit substitutes zero for the variable CntUp. On the other handwhen ID of the partner in Certificate is unregisteredone will be substituted for the variable CntUp if the variable SinkCnt is smaller in the variable SinkCnt and the variable MaxSink as compared with an ID list.

[0045]The sink 2-1 can receive contents by receiving key information and solving the code contents were enciphered using it.

[0046]Like the sauce 1 and the sink 2-2 which are shown in drawing 1when the contents outputted from the sauce 1 are received by the sink 2-2 after they go via the bridge 3-1the sink 2-2 and the bridge 3-1 perform authenticating processing as shown in drawing 5 too. That islike the sauce 1the sink 2-3or the sauce 1 and the sink 2-4even when contents are transmitted via two or more sets of bridgesthe sink 1 and the last bridge 3-2 (bridge connected sink 2-32-4 and directly) perform same authenticating processing.

[0047]The process flow of the sink 2 in the above authenticating processing is shown in drawing 6and the process flow of the sauce 1 is shown in drawing 7respectively.

[0048]The authenticating processing of the sink 1 is completely the same as the case of the sauce 2even if a partner is the bridge 3. The authenticating processing of the bridge 3 differs in the processing shown in Step S15 of drawing 7 from the case of the sauce 2. In

SinkCnt=MaxSinkspecifically the bridge 3In order to enlarge the value of the variable MaxSinkauthenticating processing which requires reception permission of the sauce 1 or the bridge 3 (if it is the bridge 3-1 in the case of the example of drawing 1 and is the sauce 1 and the bridge 3-2 bridge 3-1) which is the dispatch origin of the contents which he has received (input) is performed. The addition of one or more sets of the number of receiving is required in this case. When this authenticating processing is successfulthe processing after Step S16 of drawing 7 is continued.

[0049]Drawing 8 is a figure explaining authenticating processing in case direct continuation of the sauce 1 and the bridge 3-1 (drawing 1) is carried out.

[0050]Firstthe control section 35 of the bridge 3-1 transmits its Certificatethe variable RelCntand the variable AbsCnt to the sauce 1 (drawing 8 **). Herethe variable RelCnt expresses the number of the reception permission which wants to newly obtain the bridge 3-1and the variable AbsCnt expresses the number of the sum total of the already obtained number of permissionand the number which wants to obtain permission this time.

[0051]If this is receivedthe control section 15 of the sauce 1 will be judged when Certificate performs DSA Verify data processing which mentioned above whether it was a just thing. And authenticating processing is ended when a decision result is not just.

[0052]When continuing processingthe control section 15 of the sauce 1 investigates whether ID of the partner in Certificate is registered to its own ID listand when registeredit substitutes the variable RelCnt for the variable CntUp.

[0053]On the other handwhen ID of the partner in Certificate is unregisteredthe control section 15 of the sauce 1 substitutes the variable AbsCnt for an ID list at the variable CntUp. And the value which added the variable CntUp to the variable SinkCnt judges whether it is smaller than the variable MaxSinkand the control section 15 of the sauce 1 ends authenticating processingwhen equal.

[0054]And the control section 15 of the sauce 1 generates pseudorandom-numbers Random_challengeand transmits to the bridge 3-1 as a communication command (drawing 8 **).

[0055]The control section 35 of the bridge 3-1 will calculate an electronic signature by performing DSA Sign data processing mentioned above to the variable RelCnt and the variable AbsCnt which transmit [a value and] using its own secret key currently held at the storage parts store 36if this communication command is received. [that] The control

section 35 of the bridge 3-1 transmits the calculated electronic signature to the sauce 1 as a communication command (Response data) (drawing 8 **).

[0056]Pseudorandom-numbers Random_challenge which he sent when the control section 15 of the sauce 1 received this communication commandWhether this electronic signature's supporting received the variable RelCnt and the variable AbsCnt and DSA Verify data processing mentioned above are performedand the justification of data is judged. Howeverthe public key of the partner in Certificate received from the partner is used instead of the public key of a previous lock management organization here. And authenticating processing is ended when a decision result is not just.

[0057]When continuing processingthe control section 15 of the sauce 1It addswhen a partner's ID is unregistered to an ID list after it transmits key information required to solve the code enciphered contents as a communication command to the bridge 3-1 (drawing 8 **) and only the value of the variable CntUp makes the value of the variable SinkCnt increase.

[0058]The bridge 3-1 receives key informationand after it solves the code contents were enciphered using itit enciphers again and it outputs contents. And the control section 35 of the bridge 3-1 increases the value of the variable MaxSink only the value of the variable RelCnt.

[0059]The process flow of the bridge 3 in the above authenticating processing is shown in drawing 9and the process flow of the sauce 1 is shown in drawing 10respectively.

[0060]Like the sauce 1 and the sink 2-3 which are shown in drawing 1or the sauce 1 and the sink 2-4After going via two or more sets of bridge 3-13-2the contents outputted from the sauce 1When received by sink 2-32-4the bridge 3-1 (it is hereafter indicated as Tx bridge) which outputs contentsand the bridge 3-2 (it is hereafter indicated as Rx bridge) which receives it perform authenticating processing as shown in drawing 8 too.

[0061]The authenticating processing of Rx bridge is completely the same as the case where a partner is the sauce 1.

[0062]The authenticating processing of Tx bridge differs in the processing shown in Step S46 of drawing 10 from the case of the sauce 1. In SinkCnt+CntUp>MaxSinkspecifically Tx bridgeIn order to enlarge the value of the variable MaxSinkauthenticating processing which requires reception permission of the sauce 1 or the bridge 3 which is the dispatch origin of the contents which he has inputted is performed (in the case of the example of drawing 1the bridge 3-1 requires attestation

of the sauce 1). The addition of the above number of receiving is required in this case (SinkCnt+CntUp) (-MaxSink). When this authenticating processing is successfulthe processing after Step S50 of drawing 10 is continued.

[0063]The case where the variable RelCnt and the variable AbsCnt are transmitted apart from Certificate as other examples of processing can be considered. For examplethere is also a method of transmitting with Response shown in drawing 8 ** or the method of completely transmitting with another communication command.

[0064]In Step S15 of drawing 7or Step S46 of drawing 10when bridge 3-13-2 attests with the sauce 1 or the bridge 3 newly connectedit is not based on the result but subsequent processing also has a method which is not continued. That isnew attestation can be regarded as the thing for making successful the attestation on and after next time.

[0065]It stops further again that the sink 2 undergoes its outputand when information required to solve a code is lostas for the sauce 1 or the bridge 3only the part of the sink 2 can reduce the variable SinkCnt. For exampleif the key information of the code the sauce 1 and the bridge 3 encipher contents is changedthe sink 2 can set its own variable SinkCnt to zero.

[0066]As mentioned abovesince the sauce 1 or the bridge 3 restricted the number of receiving of the sink 2 which can undergo an outputan effect as taken below is acquired.

(1) The right holder about contents can prevent unjust viewing and listening and record of contents.

(2) Even when the re output of the signal is carried out using a bridgesauce can restrict the number also including the sink which is in the point of a bridge.

(3) By performing restriction of the number using ID peculiar to apparatuseven if the same sink attests how many timesdon't increase the number accidentally.

(4) When a bridge requires reception permission of sauce or another bridgean increase or decrement of the number of receivingand the number of the reception sum total by telling about sauce and another bridgeWhen having attested with the bridgealso in any when not having attestedthe variable SinkCnt can be easily changed into a right value.

(5) By using public-key-encryption artdevice-dependent ID and the number of a demand can be safely passed to other apparatusand number management of the right can be performed.

[0067]Although a series of processings mentioned above can also be performed by hardwarethey can also be performed by software. The

computer by which the program which constitutes the software is included in hardware for exclusive use when performing a series of processings by softwareOr it is installed in the personal computer etc. which can perform various kinds of functionsfor exampleare general-purposeetc. from a recording medium by installing various kinds of programs.
[0068]. Apart from a computerthis recording medium is distributed in order to provide a user with a program. The magnetic disk with which the program is recorded (a floppy disk is included)an optical disc (CD-ROM (Compact Disk-Read Only Memory).) . DVD (Digital Versatile Disk) is included. It is not only constituted by the package media which consist of a magneto-optical disc (MD (Mini-Disk) is included) or semiconductor memorybutIt comprises ROMa hard disketc. with which a user is provided in the state where it was beforehand included in the computer and in which the program is recorded.
[0069]In this specificationeven if the processing serially performed in accordance with an order that the step which describes the program recorded on a recording medium was indicated is not of course necessarily processed seriallyit also includes a parallel target or the processing performed individually.
[0070]In this specificationa system expresses the whole device constituted by two or more devices.
[0071]
[Effect of the Invention]As mentioned aboveaccording to the 1st information processor of this inventionthe 1st information processing methodand the program currently recorded on the 1st recording medium. Unless the number of receiving exceeds an acceptable value even if it permits the reception when contents are enciphered and reception permission is required from other devicesIt attests with other devicesand since the release key of which the code of contents is canceled was transmitted to other devices based on the authentication resultit becomes possible to restrict use of contents.
[0072]According to the 2nd information processor of this inventionthe 2nd information processing methodand the program currently recorded on the 2nd recording medium. Since the number of permission which obtained the contents which received via the 1st network from the 1st device from the 1st device was transmitted to the 2nd device via the 2nd network at the maximumit becomes possible to restrict the receiving set of output contents based on the obtained number of permission.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a block diagram showing the example of composition of the network system which applied this invention.
[Drawing 2]It is a block diagram showing the detailed example of composition of the sauce of drawing 1.
[Drawing 3]It is a block diagram showing the detailed example of composition of the sink of drawing 1.
[Drawing 4]It is a block diagram showing the detailed example of composition of the bridge of drawing 1.
[Drawing 5]It is a figure explaining the authenticating processing of sauce or a bridgeand a sink.
[Drawing 6]It is a flow chart explaining the authenticating processing to the sauce or the bridge of a sink.
[Drawing 7]It is a flow chart explaining the authenticating processing to sauce or the sauce of a bridge.
[Drawing 8]It is a figure explaining the authenticating processing of Rx bridge of sauce or Tx bridge.
[Drawing 9]It is a flow chart explaining the authenticating processing to the sauce of Rx bridgeor Tx bridge.
[Drawing 10]It is a flow chart explaining the authenticating processing to Rx bridge of sauce or Tx bridge.
[Description of Notations]
1 Sauce2-1 to 2-4 A sink3-13-2 A bridge and 11 A content player12 Media and 13 A cryptopart and 14. Communication I/F and 15 [A decoding part and 23 / Communication I/F24 control sectionsand 25 / A storage parts store and 31 / Communication I/F and 32 / A decoding part and 33 / A cryptopart and 34 / Communication I/F and 35 / A control section and 36 storage parts stores] A control section and 16 A storage parts store and 21 A picture and a voice output partand 22